

58



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/841,503	04/24/2001	Richard Alan Dayan	RPS9 2001 0011	5669

7590 08/25/2004

IBM Corporation  
Personal and Printing Systems Group  
Dept. 9CCA/Bldg. 002-2  
P.O. Box 12195  
Research Triangle Park, NC 27709

EXAMINER

HENNING, MATTHEW T

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 08/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

58

**Office Action Summary**

Application No.

09/841,503

Applicant(s)

DAYAN ET AL.

Examiner

Matthew T Henning

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 24 April 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-32 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 April 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 04/24/2001.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

Art Unit: 2131

This action is in response to the communication filed on 04/24/2001.

**DETAILED ACTION**

1. Claims 1-32 have been examined.

***Title***

2. The title of the invention is acceptable.

***Priority***

3. No claim for priority has been made for this application.
4. The effective filing date for the subject matter defined in the pending claims in this application is 04/24/2001.

***Information Disclosure Statement***

5. The information disclosure statement (IDS) submitted on 04/24/2001 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

***Drawings***

6. The drawings filed on 04/24/2001 are acceptable for examination proceedings.

***Claim Rejections - 35 USC § 102***

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

*A person shall be entitled to a patent unless –*

Art Unit: 2131

*(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.*

8. Claims 1- 4, and 13-19, 26-28 are rejected under 35 U.S.C. 102(b) as being anticipated by Gafken (U.S. Patent Number 6,026,016).

9. Claim 1 recites a method for updating a protected partition within a hard drive of a computing system, wherein said method comprises (See Gafken Fig. 5): starting execution of an initialization program in a processor within said computing system in response to turning on electrical power within said computing system (See Gafken Col. 3 Paragraph 2 Lines 1-4); determining whether an update partition file is stored in non-volatile storage (See Gafken Col. 5 Paragraph 5) within said computing system for subsequently updating said protected partition (See Gafken Col. 13 Paragraphs 4 and 7); after determining that said update partition is stored within said computing system for updating said protected partition, writing a portion of said update partition file to said protected partition (See Gafken Col. 13 Paragraph 8); and locking said protected partition to prevent further modification of information stored within said protected partition (See Gafken Col. 13 Paragraph 9 – Col. 14 Paragraph 1).

10. Claim 2 recites that a flag bit is set in non-volatile storage within said computing system when said update partition file is stored in non-volatile storage within said computing system (See Gafken Col. 13 Paragraph 4), and determining whether said update partition is stored within said computing system for updating said protected partition is performed by determining whether said flag bit is set (See Gafken Col. 13 Paragraph 7 and Fig. 5 Step 550).

Art Unit: 2131

11. Claim 3 recites that after determining that said update partition file is stored within said computing system for updating said protected partition, verifying whether said update partition file has been generated by a trusted server system, and said portion of said update partition is written to said protected partition only following verification that said update partition file has been generated by a trusted server system (See Gafken Col. 12 Paragraph 6 – Col. 13 Paragraph 1 and Figure 6).

12. Claim 4 recites that verification that said update partition file has been generated by said trusted server system includes: forming a first message digest by applying a hash algorithm to a portion of said update partition file; forming a second message digest by decrypting a digital signature within said update partition file using a public key of said trusted server system; and determining that said first and second message digests are identical (See Gafken Col. 12 Paragraph 7 Line 10 – Col. 13 Line 2).

13. Claim 13 recites a method for updating a protected partition within a hard drive of a client computing system, wherein said method comprises: generating an update partition file within a server (See Gafken Col. 12 Paragraph 7 – Col. 13 paragraph 1, wherein it was inherent that the server created the image by signing it in order for the server to be verified through digital signatures); transferring said update partition file from said server to said client computing system (See Gafken Col. 12 Paragraph 5); storing said update partition file in non-volatile storage within said client computing system (See Gafken Col. 5 Paragraph 5); starting execution of an initialization program in a processor within said client computing

Art Unit: 2131

system in response to turning on electrical power within said client computing system (See Gafken Col. 3 Paragraph 2 Lines 1-4); determining that said update partition file is stored in non-volatile storage within said client computing system (See Gafken Col. 13 Paragraphs 4 and 7); writing a portion of said update partition file to said protected partition (See Gafken Col. 13 Paragraph 8); and locking said protected partition to prevent further modification of information stored within said protected partition (See Gafken Col. 13 Paragraph 9 – Col. 14 Paragraph 1).

14. Claim 14 recites that the update partition file is transferred from said server to said client computing system by means of electrical signals transmitted through a public switched telephone network (See Gafken Col. 4 Paragraph 7 wherein it was inherent that the update file was received through the wireless transmitter, and therefore through a public switched telephone network).

15. Claim 15 recites that update partition file is transferred from said server to said client computing system by means of electrical signals transmitted over a local area network (See Gafken Col. 12 Paragraph 5).

16. Claim 16 recites that transferring said update partition file from said server to said client computing system includes: writing said update partition file to a removable computer readable medium from said server; transporting said removable computer readable medium from said sever to said client computing system; and reading said update partition file from said removable computer readable medium into said client computing system (See Gafken Col. 12 Paragraph 5 wherein it was inherent that the image was stored to a floppy disk

Art Unit: 2131

and retrieved from the floppy disk in order for the image to have been obtained through a floppy drive).

17. Claim 17 is rejected for the same reasons as claim 2 above.

18. Claim 18 is rejected for the same reasons as claim 3 above.

19. Regarding claim 19, Gafken disclosed the use of digital signatures to verify the origin of the update file (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

20. Claim 26 recites a computer system comprising: a processor executing an initialization program in response to power being turned on in said computer program (See Gafken Fig. 1 Element 110); a hard drive having a protected partition blocked during execution of an initialization program to prevent changing information stored within said protected partition (See Fig. 1 Element 130); non-volatile storage storing an update partition data structure for modifying contents of said protected partition and said initialization program, wherein said initialization program executing within said processor determines that said update partition data structure is stored in said non-volatile storage, writes a portion of said update partition data structure to said protected partition, and locks said protected partition to prevent further modification of information stored within said protected partition (See rejection of claim 1 above).

21. Claim 27 is rejected for the same reasons as claim 2 above.

22. Claim 28 is rejected for the same reasons as claim 3 above.

***Claim Rejections - 35 USC § 103***

23. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

*(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.*

24. Claims 5, 6, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gafken as applied to claims 3 and 18 above, and further in view of Schneier ("Applied Cryptography").

Gafken disclosed the use of digital signatures, including public and private keys, in order to verify that a valid server generated the boot image (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1), but Gafken did not disclose the use of a password in the signature. However, Gafken did disclose the use of password challenges.

Schneier teaches that providing a random number (password), supplied by a receiver to a sender, in a digital signature of the sender, causes the signature to be undeniable and therefore secure (See Schneier Page 81).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier to the validation signatures of Gafken by providing predetermined random number in the signature of the



Art Unit: 2131

update image. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide protection against illicitly signed updates.

25. Claims 6 and 20 recite that the data includes said version of said setup password appended to a portion of said update partition file (See rejection of claim 5 above), said algorithm is a hash algorithm generating a message digest (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1), and verifying that said update partition file has been generated by said trusted server system includes applying said hash algorithm to said setup password stored within said computing system appended to a portion of said update partition file to generate a first version of a message digest and comparing said first version of said message digest with a second version of said message digest obtained by signing said encrypted portion of said update partition file (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

26. Claims 7, 8, 22, 23, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gafken as applied to claims 1, 13, and 28 above, and further in view of Hayashi et al. (US 2001/0039651 A1) hereinafter referred to as Hayashi.

Gafken disclosed digitally signing the update file and verifying the signature prior to updating the partition (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1), but Gafken failed to disclose encrypting portions of the file separately and verifying each portion individually.

Hayashi teaches a method for providing a variety of software safely by breaking the file into pieces and decrypting each piece separately (See Hayashi Page 1 Col. 2 Paragraphs 3-10).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Hayashi to the updating system of Gafken by encrypting parts of the file separately from the other parts. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide users with customized software without imposing too much of a load on the provider.

27. Claim 8 recites forming a first message digest by applying a hash algorithm to said entry, and forming a second message digest by signing said encrypted element associated with said entry using a public key of said trusted server system, and determining that said first and second message digests are identical (See Gafken Col. 12 Paragraph 7 Line 10 – Col. 13 Line 2).

28. Claim 23 recites that each encrypted element is formed in said server by applying a hash algorithm to said entry, forming a first message digest, and by signing said first message digest with a private key of said server; and verification that said entry has been generated by said server includes forming a second message digest by applying a hash algorithm to said entry, forming a third message digest by signing said encrypted element associated with said entry using a public key of said server, and determining that said second and third message digests are identical (See Gafken Col. 12 Paragraph 7 Line 10 – Col. 13 Line 2).

Art Unit: 2131

29. Claims 9, 10, 24, 30, 31, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Gafken and Hayashi as applied to claims 7, 22 and 29 above, and further in view of the combination of Schneier.

Gafken and Hayashi disclosed the use of digital signatures, including public and private keys, in order to verify that a valid server generated the boot image parts (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1), but Gafken and Hayashi did not disclose the use of a password in the signature. However, Gafken and Hayashi did disclose the use of password challenges (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

Schneier teaches that providing a random number (password), supplied by a receiver to a sender, in a digital signature of the sender, causes the signature to be undeniable and therefore secure (See Schneier Page 81).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier to the validation signatures of Gafken and Hayashi by providing predetermined random number in the signatures of the update parts. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide protection against illicitly signed update parts.

30. Claims 10 recites that the data includes said version of said setup password appended to a said entry (See rejection of claim 5 above), said algorithm is a hash algorithm generating a message digest, and verifying that said entry has been generated by said trusted server system includes applying said hash algorithm to said setup password stored within said computing system

Art Unit: 2131

appended said entry to generate a first version of a message digest and comparing said first version of said message digest with a second version of said message digest obtained by signing said encrypted element (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

31. Claim 24 recites that a setup password is stored in non-volatile storage within said client computing system; a copy of said setup password is stored in a database accessed by said Server (See rejection of claim 5 above); said encrypted element of said update partition file is prepared in said server by signing, with a private key of said server, a result of the application of an algorithm to data including said copy of said setup password', and verification within said client computing system that said entry has been generated by said server includes signing said encrypted element associated with said entry with said public key of said server (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

32. Claim 30 recites that the non-volatile storage additionally stores a setup password, and each said encrypted element includes a digital signature signed by said trusted server system, wherein said digital signature is formed by applying a hash algorithm to an entry associated with said encrypted element to form a message digest and by signing said message digest with a private key of said trusted server system (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

33. Claim 31 is rejected for the same reasons as claim 10 above.

Art Unit: 2131

34. Claim 32 is rejected for the same reasons as claim 10 above and further because Gafken disclosed a processor (See Gafken Fig. 1 Element 110).

35. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Gafken and Hayashi as applied to claim 7 above, and further in view of Hasbun et al. (U.S. Patent Number 6,088,759) hereinafter referred to as Hasbun.

Gafken and Hayashi disclosed a method for updating a bios with a file consisting of multiple parts (See rejection of claim 7 above), but failed to disclose overwriting similar parts and appending new parts.

Hasbun teaches that a bios update can be allocated into virtual blocks so that the blocks can be updated individually without having to erase the entire memory first (See Hasbun Col. 5 Paragraph 6 – Col. 6 Paragraph 2). Hasbun also teaches that new blocks should be allocated from existing free memory (See Hasbun Col. 7 Paragraph 2).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Hasbun to the bios updating system of Gafken and Hayashi by updating each update part one at a time. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a safe method for updating a bios without risking loss of the entire bios in the event of a power failure.

36. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gafken as applied to claim 1 above, and further in view of Schmidt (U.S. Patent Number 5,826,015).

Art Unit: 2131

Gafken disclosed a secure bios updating system (See rejection of claim 1 above) but failed to disclose requiring a user to input a password to unlock the bios write capabilities. However, Gafken did disclose the use of password challenges (See Gafken Col. 12 Paragraph 7 – Col. 13 Paragraph 1).

Schmidt teaches that in order to remotely upgrade a bios, an administrator password should be provided in order to unlock the partition (See Schmidt Fig. 9 and abstract).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schmidt to the bios updating system of Gafken by requiring a correct password to be entered in order to unlock the bios altering capabilities. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the current bios from accidental or illicit alterations.

### ***Conclusion***

37. Claims 1-32 have been rejected.

38. Please direct all inquiries concerning this communication to Matthew Henning whose telephone number is (703) 305-0713. The examiner can normally be reached Monday-Friday from 9am to 4pm, EST.


If attempts to reach examiner by telephone are unsuccessful, the examiner's acting supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The fax phone number for this group is (703) 305-3718.

Art Unit: 2131

Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.



Matthew Henning  
Assistant Examiner  
Art Unit 2131

  
EMMANUEL L. MOISE  
PRIMARY EXAMINER  
A/U 2136